



The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity

Christian Leuprecht, Joseph Szeman & David B. Skillicorn

To cite this article: Christian Leuprecht, Joseph Szeman & David B. Skillicorn (2019) The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity, *Contemporary Security Policy*, 40:3, 382-407, DOI: [10.1080/13523260.2019.1590960](https://doi.org/10.1080/13523260.2019.1590960)

To link to this article: <https://doi.org/10.1080/13523260.2019.1590960>



© 2019 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 27 Mar 2019.



Submit your article to this journal [↗](#)



Article views: 3087





View related articles [↗](#)



View Crossmark data [↗](#)



The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity

Christian Leuprecht ^a, Joseph Szeman ^b and David B. Skillicorn ^c

^aDepartment of Political Science and Economics, Royal Military College, Kingston, Canada;

^bPolitical Studies, Queen's University, Kingston, Canada; ^cSchool of Computing, Queen's University, Kingston, Canada



ABSTRACT

Cyberspace is a new domain of operation, with its own characteristics. Cyber weapons differ qualitatively from kinetic ones: They generate effects by non-kinetic means through information, technology, and networks. Their properties, opportunities, and constraints are comparable to the qualitative difference between conventional and nuclear weapons. New weapons and their target sets in a new domain raise a series of unresolved policy challenges at the domestic, bilateral, and international levels about deterrence, attribution, and response. They also introduce new risks: uncertainty about unintended consequences, expectations of efficacy, and uncertainty about both the target's and the international community's response. Cyber operations offer considerable benefits for states to achieve strategic objectives both covertly and overtly. However, without a strategic framework to contain and possibly deter their use, make state and non-state behavior more predictable in the absence of reciprocal norms, and limit their impact, an environment where states face persistent attacks that nonetheless fall below the threshold of armed conflict presents a policy dilemma that reinforces collective insecurity.

KEYWORDS Cyberwarfare; cyber operations; hybrid warfare; cyber-attack; security dilemma; collective security

The nuclear bombs that devastated Hiroshima and Nagasaki did not produce quantitatively different results from earlier bombing attacks – the Allies had effectively devastated Tokyo and Dresden using conventional bombing. However, it soon became apparent that their affordances made atomic weapons qualitatively different from other weapons: less risk to attackers and small enough to be mounted on missiles. This gave rise to a new military and strategic doctrine which has proven sufficiently robust that atomic weapons have not been used since (Ruble & Cohen, 2018; Tannenwald, 1999).

Similarly, although cyber weapons can produce effects (destruction of infrastructure, rendering adversaries' weapons ineffective or inoperable)

CONTACT Christian Leuprecht  christian.leuprecht@rmc.ca  Department of Political Science and Economics, P.O. Box 17,000, Station Forces, Kingston, ON K7K 7B4, Canada

© 2019 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

that can be achieved by other means, offensive cyber weapons act differently, have different affordances, and have a different cost profile. Unlike nuclear weapons which are a last-strike capability, cyber weapons are a first-strike capability. Many states are only just starting to explore their use (or at least potential use) while simultaneously attempting to develop doctrines and rules of engagement to govern their use. In this regard, democracies distinguish themselves from other state and non-state actors by virtue of the application of a deliberate rule-of-law process. In targetting, for instance, that difference is manifest in adherence to the Geneva Convention.

Singer and Friedman (2013) survey the history of warfare in the cyber domain along with current trends. Rid (2011), Kello (2013), Liff (2012), and Stone (2012) debate the possibility, limitations, and parameters of cyberwar. As cyberwarfare strategies proliferate, comparative studies by Lewis and Katrina (2011) and Levin (2013) have exposed the scope of the proliferation of cyberwarfare strategies internationally. However, literature on cyberwarfare remains relatively limited, and on Offensive Cyber Operations (OCO) even more so. Is it even warfare when a state is constantly subject to cyber activities by adversarial state and non-state actors such as crimes, espionage, and malicious cyber activities that do not amount to an actual attack because they do not meet the threshold of armed force? The little literature there is tends not to recognize that nuance. This article draws on the existing literature on cyberwarfare and OCOs by analyzing key opportunities and constraints of OCOs and surveying the collective-security and defense implications for policy and decision makers. The article concludes that their general lack of understanding of technology notwithstanding, democratic policy makers nonetheless have an interest in encouraging the diffusion of reciprocal norms while discouraging unacceptable behavior by state and non-state actors. A fuller understanding of how OCOs contribute to collective insecurity is important for democratic policy makers to factor into their decision calculus. Because these capabilities already exist, this is not so much a problem of proliferation giving rise to a cyber security dilemma than it is of how to use cyber weapons. Navies roaming the seas does not make them less secure or contribute to proliferation per se (Nakasone, 2019). For the most part, the strategic and intelligence benefit of cyber access, disruption and denial outweighs that of destruction. Only in an actual theatre of operations during wartime does that calculus change. Absent reciprocal norms to govern acceptable behavior, however, one actor's standard cyber modus operandi runs the risk of being deemed an attack by another.

Properties of cyber weapons

Cyber weapons contain the actions of an adversary or inflict damage. However, they are qualitatively different from conventional weapons

because they operate in cyberspace, a domain with substantially different characteristics from the conventional domains of land, sea, air, and space. Like a neutron bomb, a cyber attack can inflict damage selectively and reversibly to particular parts of an adversary's environment. Cyberspace is both a technical and a human construct, rapidly changing, opaque to non-experts, and with a "geography" that is decoupled from the physical world (Cattaruzza & Danet, 2014; Cattaruzza, Daniet, & Taillat, 2018). Key properties distinguish offensive cyber weapons in terms of deterrence, attribution, and response:

- They are typically single use, that is their use will almost inevitably reveal their presence to the adversary who can then act to remove them (Gompert & Libicki, 2015). Of course, this may not matter if their (single) use is catastrophic, for example devastating critical infrastructure. (However, it is conceivable that many different variants of a cyber weapon can be developed cheaply; so, detection in one environment may not preclude continuing concealment in another.)
- They can be prepositioned in an adversary's computational infrastructure long before they might be used. However, once in place they cannot report their status without endangering their concealment; therefore, they resemble embedded ("sleeper") espionage agents. As a result, that attacker cannot be sure whether the cyber weapon remains ready to use until a signal is sent to trigger it.
- They can be used with unprecedented fine-grained control of the damage they cause. A cyber weapon can be used to demonstrate the capability to inflict damage without actually doing so; such a weapon can attack an individual target with specificity; can cause widespread (but still controlled) damage; or can destroy indiscriminately. Some kinds of attacks (blocking access to computational resources, for example) can be reversed, allowing the use of cyber weapons to be coercive in a way that oscillates between a demonstration attack and *détente* (Hare, 2018; Owens, Dam, & Lin, 2009). Fine-grained control enables aggression to be ratcheted up in smaller increments than is possible with conventional weapons.
- Attribution of the source of a cyber weapon can be difficult: It is hard for a defender to know for certain from where an attack is originating, and even more difficult to convince others, say the North Atlantic Treaty Organisation (NATO) or the United Nations (UN), of the attack's source. Still, many scholars now acknowledge that attribution is not as problematic as previously thought as the type and complexity of a target in combination with increasingly sophisticated digital forensics limit the list of likely adversaries (Kugler, 2009; Lindsay, 2015; Rid & Buchanan, 2015).
- Cyber weapons have a shelf life, because the vulnerabilities in the target system that they use may be patched as part of routine maintenance of

that system. Of course, all weapons have a shelf life, but the pace of change is much greater in the cyber domain. At the same time, attacks such as the EternalBlue exploit that was leveraged by WannaCry and NotPetya illustrates, vulnerabilities often persist for years due to poor network hygiene and failure to patch. The short-lived “transitory” nature of cyberweapons may encourage their immediate use, especially if they align with a state’s strategic interests (Gavin, 2017; Gompert & Libicki, 2015; Smeets, 2018).

- In the first instance, cyber weapons do not act in the physical universe, but in cyberspace. The combination of computing infrastructure with communication networks are, on the one hand, ubiquitous, reaching from satellites all the way down to Internet of Things (IoT) devices that are extremely small; on the other hand, they are structured with a topology that is largely unrelated to that of the globe. Until recently, some parts of cyberspace – military networks, fighter aircraft – were separated from the worldwide Internet, but these separations have been shown to be illusory both by the development of bridging “tricks” (e.g., using high-frequency audio between computers connected to the Internet and the separate network) and by the need to update software on the computers and switches on these separate networks. As a result, botnets and worms such as Code Red and NotPetya risk straying into defence or critical infrastructure by accident rather than design, but a subject of the attack sees only the capability from which (un)intent can be difficult to decypher.
- Consequently, the actions of cyber weapons do not fit with the Westphalian conception of borders in the way that kinetic weapons do. The infrastructure of global digital networks is largely owned and operated by private multinational businesses, and there is no necessary reason why traffic from A to B should follow a path that resembles the direct one – traffic may pass through other, unexpected, countries in transit and malicious diversions can be imposed by other parties with little effort. (For this reason, attempts to construct a *cyber-Westphalia* are doomed.)

Cyber weapons are the analogue of kinetic weapons – they are components of cyber operations, cyberattacks and ultimately cyberwarfare. Cyber weapons are developing rapidly, and their impact and potential are poorly understood, both at the technical and military level, especially by governments (Kello, 2017). At present, therefore, the main consequence of the existence of cyber weapons, and cyber operations, is *uncertainty*. Policy is embryonic; so, rules of engagement range from *ad hoc* to inconsistent. This is dangerous, as the late 1950s were dangerous for the Soviet Union and the United States: It would be easy for a cyber-incident to spiral out of control because of unintended consequences, with deleterious implications for collective security. However, nuclear attacks are a last strike weapon while cyber attacks might be considered a first strike weapon. Military systems are under constant

attack from sources ranging from the trivial, so-called “script kiddies,” up to other states and sophisticated non-state actors, and it is inherently difficult to separate the wheat from the chaff.

OCOs are readily conceptualized as the use of new kinds of weapons, notably in support of conventional military operations; so, it is natural that most of the thinking about them has happened within the context of militaries. Thirty-three states now include cyberwarfare in their military doctrines and a dozen states are in the process of establishing military cyberwarfare units (Lewis & Katrina, 2011). Four of the five members of the Five-Eyes community – the United States, the United Kingdom, Canada, and Australia – have or are developing tools and legislation to enable OCOs, as have France, Germany, and the Netherlands, although how exactly this works out in practice is still unclear in the public domain (Hanson & Uren, 2018; Lonsdale, 2016; Owens et al., 2009; Segal, 2017).

The Australian Strategic Policy Institute (ASPI) conceptualizes offensive cyber as operations that “manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks” (Uren, Hogeveen, & Hanson, 2018). That is against the backdrop of four other definitions

- (1) The U.S. Department of Defense defines *cyberspace* as: “A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Department of Defense, 2013, p. 5). This definition, therefore, includes weapons systems that rely on a computational infrastructure (i.e., all of them) and cyberphysical systems (electrical grid, water purification and supply), as well as the more obvious networks (Internet, telecommunications, satellites, GPS).
- (2) *Computer Network Operations* (CNO) are “actions taken to defend, exploit and/or attack information on information systems and/or the information systems themselves” (Bernier & Treurniet, 2010, pp. 229–230). They are comprised of three distinct activities: Computer Network Attack (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE) (Dittrich, 2008; Owens et al., 2009).
- (3) *Computer Network Exploitation* (CNE) is “a directed, covert activity conducted through the use of computer networks to remotely enable access to, collect information from, and/or process information on computers or computer networks” (Bernier & Treurniet, 2010, p. 230). The primary purpose of CNE is covert intelligence gathering and espionage. However, networks are almost always the best way to reach into an adversary’s environment; so, computer network exploitation acts as a vehicle for many cyber weapon attacks (Owens et al., 2009). This is not essential;

the Stuxnet attack was implemented using USB keys, since the systems being attacked were air-gapped (i.e., disconnected) from the Internet.

- (4) *Computer Network Attack* (CNA) is conducted intentionally to “disrupt, deny, degrade, or destroy adversary computers, computer networks and/or the information resident on them” (Bernier & Treurniet, 2010, p. 230).

CNAs are, of course, only one kind of OCO; the other large class of OCOs attack so-called cyberphysical systems: physical systems with an underlying computational framework that controls them. This latter class includes many different kinds of complex systems: factories, power generation and electrical grids, water purification, transportation systems, financial systems including ATMS, and many more. The banking system, for example, could be destroyed by a computer network attack, making it impossible to move financial data around, but could also be destroyed by a cyberphysical attack that cut off electrical power to a region.

Defence Cyber Operations Response Actions (DCO-RA) are deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend cyberspace capabilities or other designated systems. That concept encompasses a defensive purpose but involves taking action to disrupt or deny offensive operations, or preparations and their precursors. These often include hardening the most vulnerable aspects of the

Table 1. Significant uses of Offensive Cyber Operations internationally.

Attributed to	Type of OCO	Effect
Israel – 2007	Military – Cyber Attack	Support to airstrike against Syrian nuclear facilities
Russia – 2007	Cyber Sabotage	DDoS attack against Estonian government
Russia – 2008	Military – Cyber Attack/ Cyber Sabotage	DDoS attack to support invasion of Georgia
Kurdistan Workers Party – 2008	Cyber Sabotage	BTC oil pipeline remotely caused explosion and fire, Turkey
USA – 2010	Cyber Subversion	Stuxnet
Germany – 2012	Cyber Subversion	Targeted China’s “great firewall”
Iran – 2012	Cyber Subversion	Targeting Saudi Aramco
Russia – 2014	Military – Cyber Attack	Support to the annexation of Crimea
North Korea – 2014	Cyber Subversion	Targeting Sony Pictures Entertainment
USA – 2014	Cyber Sabotage	Targeting North Korean Internet connection
Russia – 2015	Cyber Subversion	Targeting French news network TV5
Russia – 2015	Cyber Subversion	Ukrainian power grid disruption
Russia – 2016	Cyber Propaganda	Targeting the US DNC
Australia – 2016	Cyber Subversion	Targeting ISIS financial records
USA – 2016	Cyber Subversion	Targeting ISIS digital content
USA – 2017	Cyber Subversion	Targeting North Korean intelligence agencies
Russia – 2017	Cyber Subversion	NotPetya ransomware
UK – 2017	Cyber Sabotage	Targeting ISIS propaganda networks
Russia – 2017	Cyber Subversion	Targeting Saudi power plant
USA – 2018	Cyber Subversion	Targeting the Russian Internet Research Agency

Source: Osawa (2017) and open sources.

Internet, which was not designed with security in mind. For example, systems can be scanned for computers or other simpler devices being used as botnets, specialized robust DNS servers can be created, certificate authenticity can be checked, and malware scans can be carried out. DCO-RAs are thus akin to the immune system in living things, on the lookout for problems before they have a chance to grow. Passive cyber defence, by contrast, is more akin to skin, preventing incursions in the first place. Internal defensive network operations do not raise the same issues as cyber operations that are external to the defender's network because they happen within the defender's systems and are under the defender's control. Nevertheless, its legal status is parlous: innocuous in some jurisdictions, it is regarded as problematic in others. As is common in the cyber arena, legislation and especially tested legislation lags technology.

CNE is necessarily a covert activity, "low and slow" and is primarily used by signals intelligence organizations to discover information about a potential adversary's environment, information, knowledge, and strategic thinking. Mounting an OCO creates a conflict with intelligence as it undermines access into an adversary's network infrastructure. Offensive actions, even preparatory ones, may reveal their presence and capabilities. This explains why destruction remains rare, and when it occurs outside of wartime or a theatre of operations it is to annoy rather than destroy per se, such as the Russian operation against Pentagon networks to signal displeasure with the US indictment of Russian operatives.

Technology development increases the modalities for OCOs; states and non-state actors are increasingly using them, at least experimentally; and the range of potential targets is growing, not least because more and more social and economic activity has an online component. This creates a typical arms-race environment. As OCOs become better understood and more prevalent, a merely defensive posture is no longer enough; states are leveraging OCO capabilities to achieve a range of strategic objectives. State-sponsored cyber-attacks tend to "follow incidents of international discord or conflict" (Osawa, 2017, p. 113) and thus are being used as an alternative to geopolitical conflict than physical confrontation. Table 1 summarizes serious state-sponsored cyber-attacks over the past decade and the states to which these attacks are believed to have been attributed.¹

As early as 1997, the United States employed basic information and electronic warfare operations to deceive Serbian air defenses which operated on a common telecommunications network (Kaplan, 2017). In 2007, Israel employed offensive cyber capabilities to target Syrian air defenses, spoofing radars with false information and enabling Israeli jets to carry out an airstrike undetected against a purported Syrian nuclear facility (Singer & Friedman, 2013). Russia adapted this strategy during the annexation of Crimea, deploying OCOs in support of Russian troops. It disrupted Ukrainian communications and achieved total information dominance over the region to

ensure the success of Russian military operations (Coyle, 2015). Russia is responsible for several unprecedented uses of OCOs, such as targeting a power grid in Western Ukraine, forcing it offline and plunging a quarter of a million people in the dark while deliberately enabling attribution by leaving behind so-called “calling cards” (Connell & Vogler, 2017). Exactly a month earlier bombs had disabled towers along the transmission line that supplied the bulk of electricity from Ukraine to Crimea, which had effectively been enabling Russia’s occupation. Still, the scale of cyber attack events between Russia and Ukraine is significant and poses a serious challenge for Ukrainian security and defence agencies (Kostyuk & Zhukov, 2019). Russian cyber activity in Ukraine is often mischaracterized as hybrid warfare even though Russia’s cyber operations were not necessarily timed to coincide with kinetic ones. The Federal Bureau of Investigation (FBI) indicted eighteen members of the Russian military intelligence (GRU) for interfering in the 2016 U.S. Presidential Election by using OCOs to compromise the Democratic National Committee (DNC) (Mazzetti & Benner, 2018; Swaine & Roth, 2018). This corroborates intelligence from the Dutch AIVD which disclosed that members of the Russian military (GRU) and foreign intelligence services (SVR) were identified as collaborating with the infamous hacking group known as Fancy Bear (Modderkolk, 2018).

Initially the analysis of conflict in the cyber domain was limited by the assumption that cyber operations were only capable of achieving effects in non-physical information domains. However, as our societal, military and governmental reliance on information systems increases so, too, does our understanding of how information systems connect and affect the physical world, both in a direct (SCADA, ICS systems) and indirect (media, politics, democratic processes) sense. This realization is behind the shift from information to hybrid warfare: OCOs leverage this expanded attack surface through target sets that generate effects in both the information and physical domains (Brenner, 2013; Tor, 2017). As operations in the cyber domain become more sophisticated and doctrines guiding their use mature, the risk of collateral or intentional physical damage that can be caused by OCOs grows exponentially. Precisely because the cyber domain is poorly understood, in democratic countries cyber operations are subject to many more authorizations than kinetic ones. But this is not the case for non-democratic and non-state actors. This divergence has repercussions for collective (in)security.

Opportunities and constraints

This section extends extant scholarly literature on conceptualizing OCOs. To this effect, the opportunities and constraints of OCOs are best understood in terms of three layers (Claver, 2018; Van den Berg et al., 2014):

- The technical affordances of offensive cyber weapons, in the current and developing computational and communication infrastructure: The technical layer defines what is possible both in terms of cyber weapons themselves, and the costs and constraints of developing and deploying them.
- The strategic affordances of offensive cyber weapons: How their existence and use can be leveraged to achieve state policy objectives. Claver (2018, p. 158) calls this the socio-technical layer comprising the “range of cyber activities that people are currently able to perform” and the interaction between people and the available IT systems.
- The affordances of national, supra-national, multinational corporations, and non-state actor governance to regulate cyberspace and thereby influence the layers underneath.

Technical layer

The increasing digitization of nearly every aspect of private industry, public services, critical infrastructure, social interaction and consumer services means that the scope of possible targets is vast. Computers play a role in all forms of critical infrastructure: communication, logistics, political processes (e.g., voting), infrastructure, business interactions with one another and with consumers, banking, transportation, and entertainment. Just about the only parts of society without a cyber component are those made of concrete.

Offensive cyber weapons can only be effective in settings where defenses are weak, but it is well known that cybersecurity defensive measures at all levels – government, business, critical infrastructure, and individually – are weak because, in the trade-off between security and convenience, convenience almost always wins. Cyber hygiene and timely patching of vulnerabilities are persistent struggles, partly because of a need for education, and partly because computer systems are so complex that patching one piece may break others. As a result, there are significant – and growing – vulnerabilities for OCOs to exploit (Skillicorn, Leuprecht, & Tait, 2016).

Attackers often have an advantage over defenders, since an attacker must succeed only once, while a defender must always succeed, but this asymmetry is even greater for offensive cyber weapons, because the cost to develop them is much smaller than for conventional kinetic military capabilities (Allen, 2001; Dittrich, 2008; Fasana, 2018; Hare, 2018; Owens et al., 2009; Stilgherrian, 2018). This may tempt small states and non-state actors to develop offensive cyber weapons that might coerce much larger and more sophisticated states. At present, however, offensive cyber weapons personnel with specialized skillsets are rare, even in major states (Hanson & Uren, 2018).

Developing a cyber payload is not enough – the attacker must also have the means to deliver it to its intended target. On the one hand, this advantages

states that already have a well-developed network exploitation capability (Owens et al., 2009). A recent report on the development of OCO capabilities by the U.K. Government Communications Headquarters (GCHQ) found that once authorized to develop OCOs, between 2014–2016 it GCHQ exceeded government expectations, almost doubling its OCO capabilities (Corera, 2017; Intelligence and Security Committee of Parliament, 2017). A sophisticated Science, Technology, Engineering and Mathematics (STEM) education system that generates highly qualified personnel, as well as significant financial investment in research and development, also provide an advantage (Hanson & Uren, 2018; Hare, 2018).

On the other hand, cyber weapons developed for one application can be modified and reused for others. As a result, lesser states and non-state actors may be tempted to steal OCO capabilities and reverse-engineer them. This flexibility also means that a single technique can be embodied in multiple tools aimed at different targets. By way of example, the notorious Russian hacker team known as “Fancy Bear” uses common sets of malware that are tailored operationally to match specific operating environments (Fireeye, 2017). There is also already a substantial black market in computer network exploitation tools, intended for industrial espionage and cybercrime, and some of these tools are readily adaptable to become delivery methods for offensive cyber weapons. This reduces the advantage of states with well-developed intellectual and CNE capabilities.

Strategic layer

This layer of abstraction focuses on the effect of using an offensive cyber weapon. The granularity with which such weapons can be used varies widely: Ranging from paralyzing servers and networks with Distributed Denial of Service (DDoS) attacks, disrupting or destroying functions of information infrastructure, destroying critical infrastructure such as electrical grids, water supplies or hospitals, destroying or corrupting online data, undermining or manipulating public opinion, to acting as an element of a conventional military attack against a state (Osawa, 2017).

All of these have already been deployed in a tactical way (Fasana, 2018). Per Table 1, Israel has employed offensive cyber capabilities to target Syrian air defenses; and OCOs have been employed by Australia and the U.K. against Daesh in the Middle East to disrupt its propaganda and its ability to generate financial income (Maley, 2018; Seals, 2018; Singer & Friedman, 2013). In the Crimea, Russia has employed OCOs in support of military operations to achieve near complete information dominance of the region, compromising and jamming communications systems of Ukrainian politicians and nearly all Ukrainian forces that could have posed a threat to Russian troops (Connell & Vogler, 2017; Coyle, 2015).

At a more strategic level, OCOs can be used to constrain or enhance the effects of other capabilities and strategies. Whether they can be used for deterrence, and whether the concept of deterrence is even meaningful under conditions of persistent attack, is a matter of controversy. OCOs have the advantage that costs incurred or damage caused to an adversary can be controlled so that it falls short of the generally accepted level of an armed attack, and can be even reversible (Owens et al., 2009). In his book about the Trump White House, Woodward (2018) comments that military advisers to the President were reluctant to recommend offensive cyberattacks against North Korea because they thought the U.S. itself was too poorly defended to withstand retaliatory cyberattacks, a nascent example of deterrence in the cyber domain.

To date, no direct use of OCO capabilities has resulted in the outbreak of traditional conflict, perhaps owing to uncertainties in the novelty of the attacks, the difficulty of attribution, and the reluctance of national cyber actors to retaliate when the path of escalation is unclear (Rid & Buchanan, 2015). Most importantly, however, the actions of armed forces in democratic countries are constrained by the rule of law, which translates into multiple authorities to ensure responsible and acceptable use, and safeguard against escalation. The fine-grained control of OCOs compared to conventional military force provides a way to manage escalation without the direct use of physical or military assets, whose effect in sparking conflict is much better known. In other words, instead of reacting to an escalating conflict by deploying physical military assets to a region, an OCO can be employed covertly to incur more controllable costs on the adversary, with the benefit of plausible deniability (Hare, 2018). Depending on the type of OCO employed, if there is a reduction in tension, the effects of the OCO can be reversed or scaled back.

Operations are constrained insofar as the benefits of exploitation and intelligence typically outweigh destruction outside of wartime or theatre operations. CNE aims to find and exploit vulnerabilities in computer systems and networks to observe and collect data. By contrast, DCO-RAs and OCOs aim to find and exploit vulnerabilities to destroy the functionality of computer systems and networks. CNE needs to be covert; OCOs almost inevitably become overt. Almost all OCOs require CNE capabilities to deliver the attack payload to the location where the operation is to occur. These capabilities thus risk being burned once discovered. This creates a tension between intelligence-gathering and the OCO branches (Owens et al., 2009). A similar tension exists between OCO and DCO-RA. In principle, hoarding zero-day vulnerabilities for use in an attack is crucial; in practice, convincing one's own systems to patch against vulnerabilities that may be years old is the most difficult task.

What appetite governments will have to employ OCOs unless they are able to achieve crucial strategic outcomes reliably is unclear (Hanson & Uren,

2018; Owens et al., 2009). The U.S. already fields a combatant cyber force under U.S. Cyber Command (USCYBERCOMM) with 6,200 personnel made up of 133 cyber teams and twenty-seven dedicated “combat mission forces” (Department of Defense, 2015, p. 6). There is no obvious way for smaller states to develop and maintain comparable capacity. On the one hand, smaller states must decide whether to follow this model on a smaller scale, perhaps drawing resources from other capabilities such as intelligence gathering, or increase defense budgets; or they might choose to purchase capabilities, aware that these same capabilities may be sold to others, including potential adversaries who may, as a result, have already fixed the vulnerabilities they exploit. On the other hand, some countries punch above their weight in this space because of a well-developed, informal hacker culture that can be leveraged by a government to build home-grown OCO tools and techniques.

Governance layer

Among the greatest impediments to developing a framework for the use of OCOs is that political leaders typically lack the requisite background (Kello, 2017). That is, they understand neither how they work, nor the possibilities and constraints on cyber operations. Kinetic weapons are intuitive, at least in a broad sense, in a way that cyber weapons are not, because so much of what they do is hidden in the digital environments in which they operate. At least in the West, few politicians come from a technical background that would enable them to understand the issues sufficiently deeply.

At the governance layer policy makers and actors attempting to govern the use of OCOs can benefit from the fact that offensive cyber capabilities can be difficult to attribute. Attribution is more of an “art” than a technical routine, requiring “nuanced and multi-layered process[es]” that are often based more on “intuition than evidence” (Rid & Buchanan, 2015, p. 4). While attacks by conventional weapons can usually be attributed beyond a reasonable doubt, attribution of a cyber-attack is tantamount to a verdict on the balance of probabilities. Government decision-makers will have to get used to this lower standard of evidence if they are to exercise the full range of options available. Precisely because OCOs often operate on the premise of plausible deniability, they enhance the range of foreign policy options that are available to states in pursuit of strategic objectives.

States that want to influence the development of rules governing the use of OCOs find themselves forced to develop the underlying tools and techniques, and regulatory structures and oversight mechanisms for their use. They find themselves having to understand the issues in a nuanced way and to have credibility at the bargaining table as track two diplomacy begin to lay the foundations for norms. The current framework for OCOs has largely been

forged in a *de facto* way by states such as of Russia, Iran, Israel, and the United States that have demonstrated a willingness to develop and deploy offensive cyberweapons. Although some offensive cyber-attacks are publicly known, the command and control (C2) frameworks behind their use are largely opaque.

At the international level, parlous international and legal frameworks surrounding the use of OCOs and the conduct of cyber espionage and cyber warfare pose a challenge to the governance of OCOs. Existing international treaties, charters and conventions governing the “use of force” and “armed attacks” are premised on conventional kinetic military conflicts and weapons (Belk & Noyes, 2012). These governance structures have yet to be adapted to the digital age and do not reference information warfare or the use of offensive cyber capabilities. Since they do not reach the threshold of “force” by design, vague legal language concerning terms like “use of force” and “armed attack” in the Law of Armed Conflict (LOAC), United Nations Charter, and the Universal Declaration of Human Rights (UNDHR) do not apply to OCOs. Ergo, states are not limited in their use of offensive cyber tools as long as they “do not arbitrarily deprive people of their property, security, privacy, or correspondence” or are “necessary, proportional and discrete.” Rationales that meet these requirements are easy to find (Belk & Noyes, 2012, p. 97; UN General Assembly, 1948). Articles five and six of the Budapest Convention come close to establishing at least some basic language (Maurer, 2011). They assert that signatories codify the following criminal offenses: “hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data,” in addition to the “production or distribution of any device, including computer program, with a primary purpose, which is in violation of Article 5” (Council of Europe, 2001, p. 5). Although most CNE operations are not commonly classified as offensive cyber actions, they arguably already violate both articles.

The Budapest Convention, which emerged from The Council of Europe in 2004, strives towards an international governance framework for cybercrime and is currently the only binding international treaty that governs some aspects of cybercrime in cyberspace. It has (only) 57 signatory states, including most of the major Western cyber-powers² but lacks participation by some of the other most aggressive cyber powers: Russia, China, India and Iran (Council of Europe, 2018).

Within NATO, the Tallinn Manual makes limited progress towards a unified doctrine governing cyberspace and especially cyberwarfare (Belk & Noyes, 2012; Claver, 2018; Deibert, 2013; Lewis, 2015; Owens et al., 2009). Significant gaps in the international governance of OCOs and cyberwarfare persist. For twenty years Russia has been spearheading attempts to frame rules governing international cybercrime and the conduct of cyberwarfare

at the United Nations. The United States resists such efforts, frequently voting against and refusing to support or sponsor draft resolutions on the topic of cybercrime and cyberwarfare (Maurer, 2011) out of concern that Russia's proposals effectively give license to unfettered abuse under the guise of sovereignty. Greater international support for resolutions in the cyber domain emerged in 2006 when China and the United States started to collaborate on forging governance principles (Maurer, 2011).

That OCOs are useful as a cost-effective, non-lethal and flexible method of covertly or overtly exerting power and pursuing strategic objectives, protected by difficult attribution and plausible deniability, poses a significant governance challenge. Cyber operations enable fine-grained control of offensive measures at lower financial and reputational cost and risk than conventional attacks. However, cyber systems are highly inter-connected, with a corresponding potential for spillover from an OCO and consequential collateral damage on a scale that could far exceed that of a conventional attack (Belk & Noyes, 2012; Owens et al., 2009). By way of example, Stuxnet was designed to target only a specific brand of Iranian centrifuge, and that via physical devices rather than network connections. Still, it spread to other systems, which exposed the Stuxnet malware to discovery by cybersecurity firms (Barrett, 2013; Osawa, 2017). Had its kill chain not been so specifically targeted, it might have spread across the world. Many kinds of malware check properties of the systems they attack – IP address, time zone, language settings – but may still spread unexpectedly because properties of systems do not have to match their real-world setting. For example, people use Virtual Private Networks (VPNs) to evade country restrictions on online content.

Governance at the international level needs to target the effects of cyber weapons: the use of OCOs constituting “cyber force” is the point at which there “should be no ethical distinction between the use of cyber force and any other type of attack that results in effects commensurate with the use of force” (Belk & Noyes, 2012, pp. 113–114). Were an OCO to cause physical injury or death such that conventional means of achieving the same ends would be considered a “use of force,” then that cyber operation amounts to “cyber force.” Similarly, used in a way that intended to cause physical injury or death in a manner analogous to kinetic weapons, an OCO would be deemed “cyber force.” However, this does not account for indirect physical injury or death; if a cyber-attack destroys banking services and precipitates a crime wave, are the resulting injuries a consequence of the cyber-attack? That explains why commanders of armed forces in democratic countries are loath to take a decision whose consequences might violate the Geneva Convention. The same, of course, may not be the case for cyber operations by other regime types or non-state actors.

Policy challenges: Wielding the sword of offensive cyber

Given these properties of offensive cyber weapons, and the environment in which they act, how are states to use them for strategic purposes? While some weapons naturally have binary effects, such as a single use of one that creates a state of war between source and target, other mechanisms for incremental oppositional interaction between states have been developed: probing of defense aborted before crossing a threshold, or the use of proxy states or non-state actors. The potential use and role of OCOs raises issues of detection, disruption, deterrence, attribution, and response that can be assessed against this background.

At the lowest level, state-sponsored espionage is an accepted norm in the international system, and cyberspace has been seamlessly integrated into it. For more than a century, and rapidly growing since The Second World War, SIGINT organizations have attempted to learn the intentions of adversaries by accessing their communications. As communication moved onto global communication networks, this task became easier, but new challenges were created. Intelligence collection using, say, radio communication is passive; and even tapping point-to-point communication is unambiguous. Intelligence collection on networks, though, required actions whose intentions are much more ambiguous, raising the prospect of misunderstanding. For example, accessing a nuclear power plant purely to gather intelligence could be misconstrued as an attempt to pre-position an advanced persistent threat (APT) to cause a meltdown. Detection of Chinese attempts to infiltrate the networks of nuclear power stations and public utilities in the United States, although not disruptive per se, raised concern about their putative objective or intent had they not been discovered (Greenberg, 2017; Segal, 2013). States that engage in cyber espionage using network exploitation thus increase the level of uncertainty between the states concerned.

The next step beyond the, in principle, passive process of intelligence collection, is disruption. This includes subversion and sabotage operations that rely on the difficulty of attribution but typically fall short of the definitions of use of force and so are difficult to respond to proportionally. Disruption encompasses the full range of cyber-attack operations used by states to achieve strategic objectives without crossing the threshold of an armed attack. At present these are the most common form of OCOs. Disruption undermines collective security, increases uncertainty and raises perceived threat levels. The lack of understanding of proportional response also increases the risk of unanticipated consequences, including uncontrolled escalation.

The range of activities, cost-effectiveness and non-lethality makes disruption an attractive and flexible tool for states to achieve strategic objectives (Belk & Noyes, 2012). Table 1 manifests the degree to which states are

realizing the operational benefit of disruption through OCOs: two-thirds of the operations involved disruption. Of the list of major state-sponsored uses of OCOs in [Table 1](#), which includes two cases of military cyberattack and recent operations by Five-Eyes nations against Daesh, all are at the level of disruption; about half involved cyber subversion operations.

At the level of disruption, OCOs are riskier than cyber actions that are used for detection, and face ethical, legal and operational constraints. The use of OCOs at this level appears to be reserved for cases when OCOs are necessary to achieve strategic effect of national importance and which can be conducted with plausible deniability.

The next step in the use of OCOs is for deterrence, insofar as deterrence is actually possible given the nature of persistent attack in cyberspace (Belk & Noyes, 2012). The novel property of cyber weapons is the possibility to demonstrate the existence of the potential of a cyber force operation by executing it briefly and reversibly. However, unlike nuclear deterrence, it is easy, cheap and expeditious to develop cyber force tools. As some states develop such tools, others have an incentive to reciprocate.

Deterrence is described in the Department of Defense's JP 1-02 as "the prevention of action by the existence of a credible threat of unacceptable counter-action" (Department of Defense, 2016, p. 67). It is achieved by creating conditions whereby adversaries believe that an attack will incur a response whose costs far outweigh the benefits of the attack. Deterrence presents significant challenges for policy makers. OCOs used by states for deterrence would likely constitute a level of disruption, damage and lethality equivalent to Belk and Noyes' most severe category of cyber activity. Thus the decision to develop or employ OCOs at that level should be considered commensurate with the deployment of highly destructive kinetic weapons.

Libicki (2009) highlights that deterrence in cyberspace needs to ensure that adversaries are aware that launching a cyber attack will result in a retaliatory strike. However, as this article seeks to show, the use of OCOs has evolved from solely targetting reciprocal information systems towards targets that encompass military assets and civilian critical infrastructure. Further, scholars who contend that cyber deterrence is unlikely typically also believe that cyber-warfare as a whole is unlikely. Libicki (2009) in particular perceives that the very idea of cyber deterrence is problematic because a state cannot be "crippled" in the cyber domain. This outdated view of the capabilities of offensive cyber weapons ignores the exponential pace at which cyber weapons have become increasingly destructive in a world that is increasingly reliant on information systems whose cyber security standards have been slow to adapt.

The recent spread of the NotPetya malware exemplifies the destructiveness of cyber weapons. Developed by the Russian military targeting Ukraine, Not-Petya spread rapidly across the globe, eventually causing more than \$10

billion in damage and effectively paralyzing Maersk, the Danish shipping company responsible for a fifth of the world's shipping capacity (Greenberg, 2018a, 2018b). In its review of the 2018 National Defense Strategy, the bipartisan National Defense Strategy Commission worked out the debilitating effects of a targeted cyberweapon on critical infrastructure (Edelman et al., 2018). However, the key benefit of cyber deterrence is that it need not be used in "all-or-nothing scenarios" (Stern, 2011). Cyber, then, is but one instrument along the spectrum of "cumulative deterrence" to signal that "red lines" have been crossed, but cyber lends itself to being calibrated in ways kinetic responses do not (Stern, 2011).

The use of OCOs for deterrence raises the stakes of cyber activity in which policy makers can choose to engage. The high level of disruption or damage necessary to function as a deterrent is likely to cross the threshold of cyber force, if actually used. As a result, it approximates an armed attack and the use of force. The development of OCOs for deterrence is likely to increase the proliferation of cyber tools that are capable of crossing the threshold of cyber force. Unlike nuclear weapons, however, highly destructive cyber tools are much more similar and as such are unconstrained by the concept of mutually assured destruction. The use of OCOs for deterrence bears significant risks for collective security and is likely to augment global insecurity.

Finally, the most serious OCOs can be considered in the same framework as conventional weapons, but even here there are distinctions. A cyber attack is one that takes place within cyberspace, that is, its effects are either on networks themselves or its physical effects are relatively minor. Cyber force is defined as "cyber-attacks with such substantial physical effects that they rise to a level that ought to be considered a 'use of force' or 'armed attack' under international law" (Belk & Noyes, 2012, p. 24). Cyber force differs from cyber-attack and cyber counterattack because it entails considerable "physical effects" in support of defensive or offensive objectives. At present, only a few states have the ability to conduct cyber force operations.

Several cyber events tread a fine line between cyber-attack and cyber force. Two notable ones are Israel's 2007 use of OCOs to disable Syrian air defenses to enable the Israeli air force to bomb suspected Syrian nuclear facilities and the suspected use of OCOs by the United States to disable North Korea's Internet access. Following the DPRK's cyber-attack on Sony Entertainment in 2014, the U.S. asserted that it would launch a "proportional response" (Perlroth & Sanger, 2014): North Korea's Internet went down for more than ten hours (Perlroth & Sanger, 2014). Neither event ratcheted up tensions between the states involved. However, both were meant to signal deterrence. Israel demonstrated to Syria that it had the capability to manipulate its air defenses at will and the United States leveraged its significant technological advantage over North Korea by showing that it had the capability to take an entire country off-line.

Cyberwarfare also suffers from an international governance deficit. Due to the rapid development of the cyber domain, states have not yet modified existing international treaties or established new ones to govern the conduct of cyberwarfare. States are able to write their own rules and doctrines governing the use of cyber weapons without constraints, guidance or oversight from the international community. As a result, there is considerable uncertainty not only about the dynamics between actors, but also the dynamics between actors and the wider international community.

OCOs naturally incentivize an arms race (Bendiek & Metzger, 2015; Kello, 2013; Long, 2016; Owens et al., 2009)– but to patch rather than arm because the tools already proliferate for purposes of exploitation and intelligence. Chinese scholars and analysts like to point out that, as the first country to establish cyber as a combatant command (USCYBERCOMM), the United States instigated the militarization of cyberspace (Segal, 2011). China justifies the development of advanced cyber capabilities to counterbalance the U.S. Similar to kinetic weapons, states that can develop and employ OCO capabilities strive for increasingly damaging and innovative ways of using OCOs. States with OCO capabilities have rapidly expanded the potential attack surface, including industrial control systems, critical infrastructure, and components of the democratic process from information operations to influence public discussion to voting machines (Edelman et al., 2018). This has significant implications not only for the safety and security of non-combatants that might rely on critical infrastructure but it also poses a serious threat to the stability and legitimacy of democratic institutions and processes worldwide. This has given rise to a security dilemma whereby other states have felt the need to develop OCO capabilities to defend themselves and maintain the status quo (Buchanan, 2017). This cyber security dilemma encompasses the full range of cyberwarfare policy options available to states: intrusion/detection, cyber-attack, cyber counter attack and cyber force (Belk & Noyes, 2012).

Without governance in the cyber domain, and especially with regard to OCOs, policy makers can negotiate domestic and international frameworks to manage the conduct of cyberwarfare and the use of OCOs. To this effect, there is an opportunity to constrain and shape the way that states engage in cyberwarfare in the future in the way the Law of Armed Conflict, the UN Charter, and the UN Declaration of Human Rights have done in the kinetic realm.

Since cyberspace offers few incentives to do so, current attempts to create norms for cyberspace are few and far between. The Budapest Convention on Cybercrime and Tallinn manuals are the most notable efforts by the international community, or democratic subsets of it, to create rules and norms for criminal activity and warfare in cyberspace. At the UN, attempts to govern cyberspace have been led by Russia since 1998. Although, these

attempts have been gaining momentum, they remain controversial (Maurer, 2011). Nonetheless, it is unlikely that states will negotiate a substantial international treaty in the near future due to the complexity of the cyber domain and the dichotomy that exists between states with regard to definitions and uses of cyberweapons. Cyber norms and rules are more likely to emerge within smaller regional, economic or security organizations such as NATO, G7/G20 or the BRICS before scaling up to cyber governance at the international level. The process is complicated by the rapidly changing nature of cyberspace and its increasing penetration into all aspects of everyday life and commerce.

Lack of clarity with respect to the intentions, targets and desired effects of OCOs has the potential to cause substantial instability in relations between states that engage in OCOs. In such an anarchic environment, policy makers have an incentive to use diplomacy to clarify the “rules of the game” and the thresholds for different types of cyber-attacks to provide some predictability and a level of order under conditions of conflict. An unfettered cyber security dilemma spurred by increasing state sponsored cyber-attacks could be avoided if states can reduce uncertainty of intentions behind the use of OCOs by establishing norms for their use, similar to kinetic weapons.

Risks

The current situation in cyberwarfare resembles that between the United States and the Soviet Union in the years soon after both acquired nuclear weapons. There is strong offensive potential, but great uncertainty about its use. Uncertainty has multiple forms.

Uncertainty about unintended consequences

Although cyber weapons can be, in effect, targeted by requiring them only to function in particular time zones, on particular dates, on systems with particular language choices, and so on, it is extremely difficult to anticipate all of the possible ways in which a weapon can escape its targeted domain and spread to other parts of the networked system, including the whole Internet, and so back to the attacker. (Similar issues have prevented the use of biological weapons despite substantial investment in developing them.)

Uncertainty about the target's responses

Because of the widespread lack of understanding of the operation of cyber and cyberphysical systems, the difficulty of distinguishing malice from incompetence when communication and computation systems malfunction, and the difficulty of assessing intent, the targets of OCOs cannot easily judge the

magnitude of the threat. There is at least the possibility that they will over-react, perhaps extremely. This could lead to retaliation at higher levels and so escalation, perhaps even spilling over into kinetic responses.

Uncertainty about efficacy

At the other extreme, an OCO may be unexpectedly ineffective because the target has patched the targeted vulnerability, discovered the gateway through which the attack was to be vectored, or simply has systems configured in ways that the attacker did not fully understand. Hence, attackers can never be sure that the apparent capability they possess will actually be available when needed.

Uncertainty about how the international community might respond

There is no yardstick by which the consequences to an attacker can be estimated. Up to this point, there has been no consistent international response to known OCOs. How will this change? Can an OCO be a war crime?

The world is, therefore, in a particularly fragile position with respect to OCOs – great potential to tempt the unscrupulous and unwary, low-cost opportunities for small states and non-state actors, high risks from almost any use of such operations, and no obvious way forward to mitigate these risks, develop precautionary principles or even a viable forum in which to address the issues.

Conclusion

In the 1940s and 1950s, strategic thinkers came to terms with the fact that nuclear weapons were qualitatively different from conventional weapons. They developed a new strategic framework to contain and deter their use, make state behavior more predictable, and limit their proliferation (Schelling, 1960). Similarly, offensive cyber weapons are qualitatively different from other weapons systems. Humanity needs new ways of thinking about them, plan for their use (or not), develop, maintain, and deploy them. Yet, the situation is more complex than the development of nuclear weapons because cyber weapons come in many different forms, and both they and their potential targets evolve rapidly.

The analysis in this article of opportunities and constraints for OCOs across three different layers – technical, operational and governance – provides key insights into cyber operations globally. In turn, this analysis informs the findings of this article with regard to the interaction effects between exploitation and destruction, and their use in disruption, deterrence and diplomacy.

Cyber operations offer considerable benefits for states to achieve strategic objectives covertly and overtly. Their main advantage is the granularity at which effects can be controlled, even including reversibility. The difficulty of attribution facilitates plausible deniability. As operations in offensive cyber generally fall short of the threshold of armed conflict, these properties blur the line between peace and war. Allowing a more proportionate response to conflicts may be advantageous. However, there are no treaties that express norms, and so prevent unfettered cyberattacks from triggering a conventional response.

How, then, to deploy cyber operations? What types of cyber operations can or should be used in different scenarios, or to achieve different objectives? Democratic policy makers have an interest in taking precautions that mitigate risk by encouraging the development and diffusion of reciprocal norms while discouraging unacceptable behavior that could escalate, when each new step can be incremental and unprecedentedly small. This article clarifies the classification of different types of OCOs and the democratic legitimization issues these classes of OCOs raise. In this regard, a fuller understanding of how cyber operations by non-democratic adversaries and non-state actors contribute to collective insecurity is important for democratic policy makers to factor into their decision calculus.

Notes

1. Table 1 distinguishes three types of OCOs: Cyber sabotage refers to paralyzing an information network, typically through distributed denial of service attacks and are thus largely reversible; cyber subversion is an offensive attack that has a disruptive or destructive effect on the function of a computer network or critical infrastructure; and military-cyber attack, which refers to a disruptive or destructive attack on an adversary's military assets alongside a conventional military operation (Osawa, 2017).
2. The United States, United Kingdom, Australia, Canada, The Netherlands, Germany, France, and Israel.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Christian Leuprecht (Ph.D, Queen's) is Class of 1965 Professor in Leadership, Department of Political Science, Royal Military College and Adjunct Research Professor at Charles Sturt University. He is a recipient of RMC's Cowan Prize for Excellence in Research an elected member of the College of New Scholars of the Royal Society of Canada. He is immediate past-president of the International Sociological Association's Research Committee 01: Armed Forces and Conflict Resolution, Munk

Senior Fellow at the Macdonald Laurier Institute and cross-appointed to the Department of Political Studies and the School of Policy Studies at Queen's University where he is also a fellow of the Institute of Intergovernmental Relations and the Queen's Centre for International and Defence Policy. An expert on security and defence, political demography, and comparative federalism and multilevel governance, he is regularly called as an expert witness to testify before committees of Parliament.

Joseph Szeman is an undergraduate student in Political Studies and History in his 4th year at Queen's University. His research interests are focused on hostile state actors, national security and cyberwarfare. Joseph has conducted research on offensive cyber operations in the Canadian context as a recipient of the Queen's Undergraduate Summer Student Research Fellowship (USSRF) and at the Centre for International and Defence Policy (CIDP) on Canadian counter violent extremism (CVE) policies.

David Skillicorn is Professor in the School of Computing at Queen's University, and an adjunct Professor at the Royal Military College of Canada. His research interests are in knowledge discovery, particularly for counterterrorism, law enforcement, and fraud. He has authored more than a hundred papers, and several books. His Ph.D. is from the University of Manitoba, and his undergraduate degree from the University of Sydney.

ORCID

Christian Leuprecht  <http://orcid.org/0000-0001-9498-4749>

Joseph Szeman  <http://orcid.org/0000-0003-3581-9967>

David Skillicorn  <http://orcid.org/0000-0003-0605-4029>

References list

- Allen, F. J. (2001). *CN(Eh?) - A recommendation for the CF to adopt computer network exploitation and attack capabilities* (Thesis). Canadian Forces College, Toronto.
- Barrett, T. E. (2013). Warfare in a new domain: The ethics of military cyber-operations. *Journal of Military Ethics*, 12, 4–17. doi:10.1080/15027570.2013.782633
- Belk, R., & Noyes, M. (2012). *On the use of offensive cyber capabilities: A policy analysis on offensive US cyber policy*. Boston: Harvard Kennedy School of Government.
- Bendiek, A., & Metzger, T. (2015). *Deterrence theory in the cyber-century lessons from a state-of-the-art literature review* (Working Paper). Berlin: German Institute for International and Security Affairs.
- Bernier, M., & Treurniet, J. (2010). *Understanding cyber operations in a Canadian strategic context: More than CAISR, more than CNO*. Paper presented at the Conference on Cyber Conflict, Tallinn, Estonia.
- Brenner, J. F. (2013). Eyes wide shut: The growing threat of cyber attacks on industrial control systems. *Bulletin of the Atomic Scientists*, 69(5), 15–20. doi:10.1177/0096340213501372
- Buchanan, B. (2017). *The cyber security dilemma: Hacking, trust and fear between nations*. Oxford: Oxford University Press.
- Cattaruzza, A., & Danet, D. (2014). *La Cyberdéfense. Quel territoire, quel droit?* Paris: Economica.
- Cattaruzza, A., Daniet, D., & Taillat, S. (2018). *La Cyberdéfense. Politique de l'espace numérique*. Paris: Armand Collin.

- Claver, A. (2018). Governance of cyber warfare in the Netherlands: An exploratory investigation. *The International Journal of Intelligence, Security and Public Affairs*, 20, 155–180. doi:10.1080/23800992.2018.1484235
- Connell, M., & Vogler, S. (2017). *Russia's approach to cyber warfare*. Retrieved from <http://www.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf>
- Corera, G. (2017). GCHQ cyber-spies 'over-achieved' say MPs. *BBC*. Retrieved from <https://www.bbc.com/news/technology-42425960>
- Council of Europe. (2001). *Convention on cybercrime*. Retrieved from <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>
- Council of Europe. (2018). *Chart of signatures and ratifications of treaty 185*. Retrieved from https://www.coe.int/en/web/conventions/full-list//conventions/treaty/185/signatures?p_auth=vFhr6vmR
- Coyle, J. (2015). Russia has complete information dominance in Ukraine. *Atlantic Council*. Retrieved from <http://www.atlanticcouncil.org/blogs/ukrainealert/russia-has-complete-informational-dominance-in-ukraine>
- Deibert, R. (2013). *Canada and the challenge of cyberspace governance and security*. Calgary: University of Calgary School of Public Policy.
- Department of Defense. (2013). *Joint publication 3-12: Cyberspace operations*. Retrieved from https://fas.org/irp/doddir/dod/jp3_12r.pdf
- Department of Defense. (2015). *The DoD cyber strategy*. Retrieved from http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf
- Department of Defense. (2016). *Joint publication 1-02: Department of defense dictionary of military and associated terms*. Retrieved from https://fas.org/irp/doddir/dod/jp1_02.pdf
- Dittrich, D. (2008). *On the development of computer network attack capabilities*. Washington, DC: National Research Council.
- Edelman, E., et al. (2018). *Providing for the common defence: The assessment and recommendations of the national defence strategy commission*. Washington, DC: United States Institute of Peace.
- Fasana, K. G. (2018). Another manifestation of cyber conflict: Attaining military objectives through cyber avenues of approach. *Defence Studies*, 18, 167–187. doi:10.1080/14702436.2018.1462661
- Fireeye iSight Intelligence. (2017). *APT28: At the centre of the storm: Russia strategically evolves its cyber operations*. Retrieved from https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html
- Gavin, F. (2017). Crisis instability and preemption: The 1914 railroad analogy. In G. Perkovich, & A. E. Levite (Eds.), *Understanding cyber conflict: Fourteen analogies* (pp. 111–122). Washington, DC: Georgetown University Press.
- Gompert, D., & Libicki, M. (2015). Cyber warfare and sino-American crisis instability. *Survival*, 56(4), 7–22. doi:10.1080/00396338.2014.941543
- Greenberg, A. (2017). Hackers gain direct access to US power grid controls. *Wired*. Retrieved from <https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/>
- Greenberg, A. (2018a). The untold story of notPetya, the most devastating cyberattack in history. *Wired*. Retrieved from <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

- Greenberg, A. (2018b). The white house blames Russia for notPetya, the “most costly cyberattack in history”. *Wired*. Retrieved from <https://www.wired.com/story/white-house-russia-notpetya-attribution/>
- Hanson, F., & Uren, T. (2018). *Policy brief: Australia’s offensive cyber capability*. Retrieved from <https://www.aspi.org.au/report/australias-offensive-cyber-capability>
- Hare, F. (2018). Precision cyber weapon systems: An important component of a responsible national security strategy? *Contemporary Security Policy*.
- Intelligence and Security Committee of Parliament. (2017). *Annual report 2016–2017*. London. Retrieved from <http://isc.independent.gov.uk/committee-reports/annual-reports>
- Kaplan, F. (2017). *Dark territory: The secret history of cyber war*. New York: Simon & Schuster.
- Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38, 7–40. doi:10.1162/ISEC_a_00138
- Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT: Yale University Press.
- Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution*, 63(2), 317–347. doi:10.1177/0022002717737138
- Kugler, R. (2009). Deterrence of cyber attacks. In F. D. Kramer et al (Ed.), *Cyberpower and national security*. Dulles: National Defense University Press and Potomac Books, Inc. chapter 13. <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-13.pdf?ver=2017-06-16-115053-773>
- Levin, A. (2013). *Securing cyberspace: A comparative review of strategies worldwide*. Toronto, ON: Privacy and Cyber Crime Institute, Ryerson University.
- Lewis, A. J. (2015). *The Tallinn papers: The role of offensive cyber operations in NATO’s collective defence*. Retrieved from <https://ccdcoe.org/multimedia/role-offensive-cyber-operations-natos-collective-defence.html>
- Lewis, A. J., & Katrina, T. (2011). *Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organisation*. Washington, DC: Centre for Strategic and International Studies.
- Libicki, M. (2009). Cyberdeterrence and cyberwar. *RAND Corporation*. Washington, DC. Retrieved from <http://www.rand.org/pubs/monographs/MG877.html>
- Liff, A. (2012). Cyberwar: A new “absolute weapons”? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, 35, 401–428.
- Lindsay, J. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, 1(1), 53–67.
- Long, A. (2016). A cyber SIOP? Operational considerations for strategic offensive cyber planning. *Journal of Cyber Security*, 3(1), 19–28. doi:10.1093/cybsec/tyw016
- Lonsdale, D. J. (2016). Britain’s emerging cyber-strategy. *The RUSI Journal*, 161, 52–62. doi:10.1080/03071847.2016.1232880
- Maley, P. (2018). Australia’s world-class cyber warriors take the fight to Islamic state. *The Australian*. Retrieved from <https://www.theaustralian.com.au/national-affairs/defence/australias-worldclass-cyber-warriors-take-the-fight-to-islamic-state/news-story/1c4d7c17c3cbc7435ad316077974ec59>
- Maurer, T. (2011). *Cyber norm emergence at the United Nations: An analysis of the activities at the UN regarding cyber-security*. Boston, MA: The Belfer Center for Science and International Affairs.

- Mazzetti, M., & Benner, K. (2018). 12 Russian agents indicted in mueller investigation. *New York Times*. Retrieved from <https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html>
- Modderkolk, H. (2018). Hackers AIVD leverden cruciaal bewijs over Russische inmenging in Amerikaanse Verkiezingen. *De Volkskrant*. Retrieved from <https://www.volkskrant.nl/nieuws-achtergrond/hackers-aivd-leverden-cruciaal-bewijs-over-russische-inmenging-in-amerikaanse-verkiezingen~b32c6077/>
- Nakasone, P. M. (2019). A cyber force for persistent operations. *Joint Forces Quarterly*, 92, 10–14.
- Osawa, J. (2017). The escalation of state sponsored cyberattack and cyber security affairs: Is strategic cyber deterrence the key to solving the problem? *Asia-Pacific Review*, 24, 113–131. doi:10.1080/13439006.2017.1406703
- Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, policy, law, and ethics regarding U.S. Acquisition and use of cyberattack capabilities*. Retrieved from http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf
- Perlroth, N., & Sanger, E. (2014). North Korea loses its link to the internet. *New York Times*. Retrieved from <https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html>
- Rid, T. (2011). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32. doi:10.1080/01402390.2011.608939
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38, 4–37.
- Ruble, R. M., & Cohen, A. (2018). Nuclear norms in global governance: A progressive research agenda. *Contemporary Security Policy*, 39, 317–340. doi:10.1080/13523260.2018.1451428
- Schelling, T. C. (1960). *The strategy of conflict*. Cambridge, MA: Harvard University Press.
- Seals, T. (2018). UK launches offensive cyber-weapons against Islamic state. *Infosecurity Magazine*. Retrieved from <https://www.infosecurity-magazine.com/news/uk-launches-offensive-cyberweapons/>
- Segal, A. (2011). Ideas about China's cyber command. *Council on Foreign Relations*. Retrieved from <https://www.cfr.org/blog/ideas-about-chinas-cyber-command>
- Segal, A. (2013). The code not taken: China, the United States, and the future of cyber espionage. *Bulletin of the Atomic Scientists*, 69, 38–45. doi:10.1177/0096340213501344
- Segal, A. (2017). Europe is developing offensive cyber capabilities. The United States should pay attention. *Council on Foreign Relations*. Retrieved from <https://www.cfr.org/blog/europe-developing-offensive-cyber-capabilities-united-states-should-pay-attention>
- Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press.
- Skillicorn, D. B., Leuprecht, C., & Tait, V. (2016). Beyond the castle model of cyber-security. *Government Information Quarterly*, 33, 250–257. doi:10.1016/j.giq.2016.01.012
- Smeets, M. (2018). Integrating offensive cyber capabilities: Meaning, dilemmas, and assessment. *Defence Studies*, 18(4), 395–410. doi:10.1080/14702436.2018.1508349
- Stern, E. (2011). Retaliatory deterrence in cyberspace. *Strategic Studies Quarterly*, 5, 62–80.

- Stilgherrian. (2018). Cyber dam busters could give Australia's military an asymmetric edge. *ZDNet*. Retrieved from <https://www.zdnet.com/article/cyber-dam-busters-could-give-australias-military-an-asymmetric-edge/>
- Stone, J. (2012). Cyber war will take place!. *Journal of Strategic Studies*, 36(1), 101–108. doi:10.1080/01402390.2012.730485
- Swaine, J., & Roth, A. (2018). US indicts 12 Russians for hacking DNC emails during the 2016 election. *The Guardian*. Retrieved from <https://www.theguardian.com/us-news/2018/jul/13/russia-indictments-latest-news-hacking-dnc-charges-trump-department-justice-rod-rosenstein>
- Tannenwald, N. (1999). The nuclear taboo: The United States and the normative basis of nuclear non-use. *International Organization*, 53, 433–468. Retrieved from <http://www.jstor.org/stable/2601286>
- Tor, U. (2017). 'Cumulative deterrence' as a new paradigm for cyber deterrence. *Journal of Strategic Studies*, 40(1–2), 92–117. doi:10.1080/01402390.2015.1115975
- UN General Assembly. (1948). *Universal Declaration of Human Rights*. 217 A (III). Retrieved March 5, 2019, from <https://www.refworld.org/docid/3ae6b3712c.html>
- Uren, T., Hogeveen, B., & Hanson, F. (2018). *Defining offensive cyber capabilities*. Retrieved from <https://www.aspi.org.au/report/defining-offensive-cyber-capabilities>
- Van den Berg, J., van Zoggel, J., Snels, M., van Leeuwen, M., Boeke, S., van de Koppen, L., ... de Bos, T. (2014). *On (the emergence of) cyber security science and its challenges for cyber security education*. Retrieved from <https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf>
- Woodward, R. (2018). *Fear: Trump in the White House*. New York, NY: Simon & Schuster.